RSA 密码破译报告

冯古豪

PKU EECS

2022 年 6 月 9 日

1. RSA 加密原理

2. 攻击方式和实验结果
   - 基于低加密指数的攻击
   - 维纳攻击
   - 基于大数分解的攻击
   - 其他攻击方式
   - 实验结果汇总

欧拉定理

定理

a, n 为两个互素的正整数，则 $a^{\phi(n)} \equiv 1 \mod n$，其中 $\phi(n)$ 为欧拉函数。

RSA 加密

RSA 加密算法首先生成出两个大素数 p, q，要加密的二进制数记为 m，公共模数 $n = pq$，公钥 e 为任意一个小于 $\phi(n)$ 的正整数。私钥 d 满足 $e \times d \equiv 1 \mod \phi(n)$，加密后我们发送的数字 $c = m^e \mod n$。在解密时，有 $m = c^d \mod n$，其中，公钥为 c 公开的，私钥 d 只有通信两方掌握。

低加密指数攻击

- 针对加密指数 e 很小的情况，一般为 2,3
- 即使 e 很小，一般也不起作用

算法原理

$m = \sqrt[e]{kn + c},\ k \in N$

枚举 k 的取值来破解 RSA

实验结果

算法的时间复杂度过高，所以无法破译出任何一组数据。

低加密指数广播攻击

- 中国剩余定理
- 相同的 m, e，多个模数 n

算法原理

$m^e = \Sigma_{i=1}^{k} c^{(i)} t^{(i)} N^{(i)} + KN$
直接枚举 K 来完成破译

实验结果

由于实验数据基本上满足 $m \sim \Theta(n)$，所以枚举的 K 的范围接近 $\mathcal{O}(n^{e-k})$，为了得到有效的时间复杂度，该算法所需要数据的组数 k 需要满足 $k \geqslant e$。运用这个方法，我成功破译了 $e = 5$ 的五组数据。

Corper-Smith 攻击

- 针对 $e = 3$ 的情形，并且知道明文 m 的高位。

算法原理

$$m = M + x$$

$$(M + x)^3 - c \equiv 0 \mod n$$

利用 Copper-Smith 算法，我们在较小的时间复杂度内解出满足条件 $x^3 - c \equiv 0 \mod n$ 的最小的 x。

实验结果

利用 Copper-Smith 算法，破译了 $e = 3$ 的 3 组数据。

维纳攻击

算法原理

$$G = \mathsf{gcd}(p-1, q-1), \lambda(n) = \frac{\phi(n)}{G}$$

$$ed = \frac{K}{G}\phi(n) + 1$$

$$\frac{e}{n} = \frac{k}{dg}\frac{\phi(n)}{n} + \frac{1}{dn}$$

用 $\frac{e}{n}$ 的连分数展开逼近 $\frac{k}{dg}$ 求得 $\phi(n)$

维纳攻击

定理 (Legendre)

若满足 $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$，$(p, q) = 1$，则 $\frac{p}{q}$ 是 α 的连分数逼近。

定理 (维纳攻击)

当数据满足 $q < p < 2q$，$d < \frac{1}{3}n^{\frac{1}{4}}$ 的条件下，维纳攻击一定能够解出 p, q。

实验结果

在本次实验的数据中，数据均没有满足维纳攻击的条件，所以我使用维纳攻击没有破译出任何数据。

费马分解

算法原理

费马分解是一种常见的大数分解的算法，由于 $n = pq$，p, q 均为素数。不妨假设 $p \geqslant q$，这时，我们有 $n = (a-b)(a+b)$，$p = a+b$，$q = a+b$，从而有 $a^2 = n + b^2$。

实验结果

- $a = \sqrt[2]{n+b^2}$，我们可以枚举 b，来完成费马分解。
- $b = \sqrt[2]{a^2 - n}$，我们可以从 $a = \lceil \sqrt{n} \rceil$ 枚举，每次加一，来完成费马分解。

我分别尝试了两种实现方式，发现前者在有效的时间内只能够破译 1 组数据，但是后一种实现方式能够破译 3 组数据。

Pollard-$p-1$ 分解

算法原理

引理 (Pollard-$p-1$)

假设 $n=pq$ 满足 $(p-1)|B!$ 且 p,q 均为素数，则令 $a=2^{B!} \mod n$，$p=\gcd(a-1,n)$。

Pollard-$p-1$ 算法先设置一个较大的 B，然后计算出 $B!$，a，然后计算 $\gcd(a,n)$ 即可，若 $\gcd(a,n)\neq 1$，则我们解出了 n 的一个素因数 p，而后用 $q=n/p$ 即可分解 n。若 $\gcd(a,n)=1$，则算法无效。

实验结果

在实验中，我将 B 的大小设置成了 200000，而后针对每一组数据的 n 分别计算 a，最终成功破译了 3 组数据。

Pollard-ρ 分解

算法原理

算法随机生成两个数 y, c，然后我们不断更新迭代 $y = f(y) = y^2 + c \mod n$，在 y 的迭代过程中，在模 n 的意义下是最终会构成一个环。然后利用 $n = pq$，完成对 n 的分解。并且我们注意到 $|f(i) - f(j)| = |i + j| \times |i - j|$，从而如果 $|i - j| \equiv 0 \mod n$，则 $|f(i) - f(j)| \equiv 0 \mod n$。所以如果环上某一些距离 d 的两个点满足 $p \mid |i - j|$ 则环上任意两个距离为 d 的点满足要求。

Pollard-ρ 分解

Floyd 算法

在判定环的过程中，我使用 Floyd 算法，开始随机生成三个数 x, y, c，迭代过程中，x 没迭代一次，y 迭代两次，并计算 $|x - y| \mod n$ 与 n 公因数，直到找到 n 的非平凡因子。

实验结果

该算法的复杂度比较依赖于随机数生成器的随机性，算法期望复杂度为 $\mathcal{O}(n^{\frac{1}{4}} \log n)$。在实验中，Pollard-ρ 算法成功破译了三组数据。

公因数分解

算法原理

对于多组数据中的不同的 n，尝试将它们两两之间求最大公因数，若存在两组 n 之间存在在非平凡的公因数，则这两组数据可以直接破译了。

实验结果

存在两组数据的 n 之间有非平凡的公因数。

共模攻击

定理 (共模攻击)

记 s, t 满足 $se^{(1)} + te_2 = 1$，则 $m \equiv (c^{(1)})^s (c^{(2)})^t \mod n$

算法原理

首先利用欧几里得算法计算出 s, t，计算出 $(c^{(1)})^s (c^{(2)})^t \mod n$ 即可。

实验结果

成功破译了两组数据。

实验结果汇总

- 一共破译了 17 组数据
- 低加密指数广播攻击数据 4，5，7，13，18
- 费马分解数据 8，10
- 公因数分解数据 2，19
- Pollard-$p-1$ 数据 1，3，12
- 共模攻击数据 11，14
- Copper-Smith 数据 0，6，17
- Pollard-ρ 数据 3，12

谢谢大家